UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/549,551	04/14/2000	Takayuki Hasebe	1341.1044/JDH	9207

21171 7590 12/08/2004

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/549,551	HASEBE ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication..
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 April 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 and 3-17 have been examined. The applicant in the amendment filed on November 17, 2004 has amended claims 1, 6, 12, 13, and 15, and added new claim 17. Claim 2 was canceled in a previous amendment.

Response to Amendment

2. The objection to claim 3 is withdrawn as the amended claim now refers to pending claim 1.

3. The rejections under 35 U.S.C. 112, second paragraph to claims 1, 12, 13 and 15 are withdrawn as the amendments to the claims overcome the 112 rejection.

Response to Arguments

4. Applicant's arguments with respect to amended claims 1 and 2-17 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

5. Claim 1 is objected to because of the following informalities: "connection date" should be "connection data". Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 3, 10, 11 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford U.S. Patent No. 5,189,700 (hereinafter Blandford) in view of Hartman, Jr. U.S. Patent No. 5,444,780 (hereinafter Hartman).

8. As per claim 1, Blandford discloses a signature creating apparatus which creates a digital signature (see Blandford, 7:17-22), the signature creating apparatus comprising:

a. a clock presenting time information (see Blandford, fig. 1, ref. no. 13);

b. an ID storing unit which stores an apparatus ID for specifying the creating apparatus using a form capable of preventing interpolation (see Blandford, 5:37-54, esp. 5:37-41; 6:4-7);

c. a personal identification storing unit which stores personal identification information (see Blandford, fig. 1, ref. nos. 8 and 10; 7:17-38);

d. a connection unit which creates connection data by connecting plain-text, the time information, the apparatus ID, and the personal identification information

that identifies a person using the creating apparatus to create the digital signature (see Blandford, fig. 1 and related text; 7:16-22; 7:39-65); and

e. a signature creating unit which creates the digital signature using the connection data created by the connecting unit and a key used only for creating a signature (see Blandford, 7:27-54, esp. 7:36-37),

f. wherein the personal identification information is stored within the signature creating apparatus using a form capable of preventing interpolation, and the signature creating unit encrypts the connection data to create the digital signature (see Blandford, 7:25-55).

2. Further, Blandford, discloses the clock is to be resettable only under a carefully prescribed procedure and by an operator with knowledge of the correct password to update the clock, but does not elaborate on the authority of the operator. See Blandford, 6:25-54. Hartman teaches a timekeeping authority system wherein a trusted time authority initializes the timekeeping facilities of its clients. See Hartman, 2:65-4:10, esp. 2:65-3:17. It would be obvious to one of ordinary skill in the art at the time the invention was made for the time information to only be set by a time authentication authority. Motivation to combine includes, inter alia, ensuring only a trusted time authentication authority updates the clock used in the signature creation steps as taught by Hartman. Ibid.

3. Further, Blandford does not expressly disclose the personal identification information specifies a person who has a proper right to update stored contents. However, it is notorious in the art for personal identification information to specify a

person who has a proper right to update stored contents. For example, in the UNIX operation system, users are assigned a UID that specifies access rights to update stored information including: user password and file access privileges on personal files. It would be obvious to one of ordinary skill in the art at the time the invention was made for the personal identification information to specify a person who has a proper right to update stored contents. Motivation to combine includes, inter alia, mapping a user identifier with a typical user role as known to one of ordinary skill in the art.

4. Finally, Blandford does not expressly disclose connecting the digital signature to the time information, the apparatus ID, and the personal identification information to create a signal data to be transmitted to a network. However, Blandford teaches making available to the user the original data used to create the digital signature. See Blandford, 4:38-44. It would be obvious to one of ordinary skill in the art at the time the invention was made to append the digital signature to the original information, thereby creating a signal data, which the user can use to verify the created signature as taught by Blandford. Ibid. Finally, Blanford discloses transmitting the created signal data to an external communication port. See Blandford, 5:29-34, 6:21-24, 7:34-38 and 7:49-55. The aforementioned cover the limitations of claim 1.

5. As per claim 3, Blandford covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the apparatus further comprises:

g. a storage unit which stores the personal identification information (see Blandford, 5:55-6:4; 7:23-38);

h. a judging unit which judges as to whether or not a person who updates stored contents of the storage unit is a person who has proper right (see Blandford, 6:41-43); and

i. an updating unit which updates the stored contents of the storage unit only when the judging unit has judged that the person who updates is the person who has proper right (see Blandford, 6:41-53).

The aforementioned cover the limitations of claim 3.

6. As per claim 10, Blandford covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the apparatus further comprises a setting unit which sets the time information according to a time setting request, the setting unit being installed in the time authentication authority. See Hartman, fig. 2, ref. no. 224 and related text; 3:46-4:10; 4:64-5:36. The aforementioned cover the limitations of claim 10.

7. As per claim 11, Blandford covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the apparatus further comprises a correcting unit, which corrects the clock automatically, the correcting unit being installed in the time authentication authority. See Hartman, fig. 2, ref. no. 224 and related text; 3:4-9, 3:34-62. The aforementioned cover the limitations of claim 11.

8. As per claim 17, it is an apparatus claim corresponding to claim 1 and it does not teach or define above the information claimed in claim 1. Therefore, claim 17 is

rejected under Blandford in view of Hartman for the same reasons set forth in the rejection of claim 1.

9. Claims 5 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman, and further in view of Fisher U.S. Patent No. 5,422,953 (hereinafter Fisher).

10. As per claim 5, Blandford covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Blandford does not expressly teach creating a digital signature only when the confirming unit confirms that the clock works normally. Fischer discloses a personal date/time notary device wherein the device comprises a confirming unit that confirms a working state of the clock and creates a digital signature only when the confirming unit confirms that the clock works normally. See Fischer, 4:42-63, esp. 4:46-48. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Fischer to the apparatus of Blandford. Motivation to combine includes, inter alia, preventing the creation of faulty digital signatures based on an invalid timestamp as taught by Fischer. Ibid. The aforementioned cover the limitations of claim 5.

11. As per claim 8, Blandford covers an apparatus as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). In addition, the confirming unit confirms the working

state of the clock based on a result of comparing a time-counted result of the clock before certain time and a time-counted result at current time. See Fischer, 4:64-5:29.

12. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman, and further in view of Ugon U.S. Patent No. 4,295,041 (hereinafter Ugon).

13. As per claim 4, Blandford covers an apparatus as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Blandford does not expressly state where the apparatus ID is stored; however, the only possible storage locations are either the RAM or the PROM. See Blandford, fig. 1, ref. nos. 10 and 12. Further, it is well known in the art for sensitive information to be stored in read-only memory to prevent modification of sensitive information. For example, Ugon discloses an apparatus wherein the sensitive information is stored in the PROM. See Ugon, fig. 1, ref. no. 2 and related text. It would be obvious to one of ordinary skill in the art at the time the invention was made for the apparatus ID to be stored in an unrewritable storage unit. Motivation to combine, includes, inter alia, ensuring the ID is not tampered with after it is initially stored as known to one of ordinary skill in the art and as taught by Ugon. Ibid. The aforementioned cover the limitations of claim 4.

14. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman and Fischer, and further in view of Boll U.S. Patent No. 4,230,958 (hereinafter Boll).

15. As per claim 7, Blandford covers an apparatus as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). Blandford is silent on the matter of confirming the working state of the clock based on a result of comparing a driving voltage of the clock with a threshold. However, in the analogous art of semiconductor detector circuits, Boll teaches an invention wherein the working property of a clock is determined by comparing the voltage of the clock with a threshold value. See Boll, Abstract; 1:23-44. It would be obvious to one of ordinary skill in the art at the time the invention was made to confirm the working state of the clock based on a result of comparing a driving voltage of the clock with a threshold. Motivation to combine includes, inter alia, enabling determination of proper clock operation based on a sample measurement of the clock's driving voltage as taught by Boll. Ibid. Moreover, this clock confirmation is distinct from other clock confirmation steps in that it checks if the clock is properly furnishing expected periodic pulses. See Boll, 1:35-40. The aforementioned cover the limitations of claim 7.

16. Claims 13 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman, and further in view of Oishi U.S. Patent No.

6,298,153 (hereinafter Oishi) and EAS "The Arithmetic and Logic Unit (ALU)" (hereinafter EAS).

17. As per claim 15, Blandford covers an apparatus as outlined above in the claim 3 rejection under 35 U.S.C. 103(a). Blandford does not teach a signature verification routine incorporated in the digital signature apparatus. Oishi discloses a device that includes a digital signature generating unit and a digital signature verification unit, which verifies interpolation using the digital signature, the plaintext and a key. See Oishi, fig. 2, ref. no. 30; 11:58-12:2; 12:41-42. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement a signature verification unit in the digital signature apparatus wherein the verification unit verifies interpolation using the digital signature, the plaintext, and a key. Motivation to combine includes inter alia, enabling the creator of the signature to verify a signature it has created.

18. Further, Oishi does not specify a function selecting switch which controls the operation of the signature verification and creation modes of the apparatus. However, the implementation of a switch to specify an active operating mode is a conventional feature of any mechanized apparatus having a plurality of modes. For example, in the analogous art of computer logic design, EAS teaches a mode select enabler to make active an operating mode in an ALU having a plurality of modes. See EAS, 2nd and 3rd figures and related text. It would be obvious to one of ordinary skill in the art at the time the invention was made for the invention disclosed by Blandford to implement a function selecting switch which controls the operation of the signature verification and creation

modes of the apparatus. Motivation to combine includes, inter alia, providing creation and verification services in one device, and the means to select between the two services as known to one of ordinary skill in the art and as taught by EAS. Ibid. Finally, the invention disclosed by Oishi includes a receiving unit that receives the plaintext to which the digital signature is connected. See Oishi, fig. 2. The aforementioned cover the limitations of claim 15.

19. As per claim 13, it is an apparatus claim corresponding to claim 15 and it does not teach or define above the information claimed in claim 15. Therefore, claim 13 is rejected under Blandford in view of Hartman, Oishi, and EAS for the same reasons set forth in the rejection of claim 15.

20. Claims 12, 14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman, Oishi, and EAS, and further in view of Schneier Applied Cryptography 2nd Edition (hereinafter Schneier).

21. As per claim 16, Blandford covers a signature apparatus as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). In addition, the switching unit switches a function as a lower apparatus and a function as an upper apparatus; and a key generating unit that generates a key used only for verification of the signature based on an apparatus ID for specifying another signature apparatus which is the lower apparatus and where the signature creating function is made effective when the key generating

unit is switched so as to function as the upper apparatus by the switching unit and the signature verification function is made effective by the function selecting unit. See Oishi, fig. 2 and related text as modified by EAS, 2nd and 3rd figures and related text.

22. Further, the apparatus implements a public key methodology and not a common key method as specified in the applicant's claim. See Blandford, 6:4-7. However, common key methods to sign and verify messages are well-known in the art. For example, Schneier teaches a method to sign documents using symmetric cryptosystems. See Schneier, pgs. 35-37, 'Signing Documents with Symmetric Cryptosystems and an Arbitrator'. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the digital signature methodology to be based on common key techniques. Motivation to combine includes, inter alia, implementing a standard digital signature methodology. See Schneier, pg. 36, characteristics 1-5. The aforementioned cover the limitations of claim 16.

23. As per claim 14, Blandford covers an apparatus as outlined above in the claims 13 and 16 rejections under 35 U.S.C. 103(a). Blandford does not disclose a key-generating unit, which receives cryptographic information about encrypting the key only for verification of the signature and decoding the cryptographic information so as to generate the key only for verification of the signature. However, as taught by Schneier in a separate section, keys are typically encrypted when transferred from a KDC to hide the keys from 3rd parties. See Schneier, pg. 176, 'Transferring Keys', 'Key-Encryption Keys'. This encrypted key method requires cryptographic information to be sent to the

receiver, namely the encrypted key, whereby the cryptographic information is used to generate the key. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the key generating unit to receive cryptographic information to generated the key for verification. Motivation to combine includes, inter alia, dynamically generating a key when requested as taught by Schneier. Ibid. The aforementioned cover the limitations of claim 14.

24. As per claim 12, it is an apparatus claim covered by the invention covered in the claim 16 rejection and it does not teach or define above the information defined in the invention as outlined in the claim 16 rejection. Therefore, claim 12 is rejected under Blandford in view of Hartman, Oishi, EAS, and Schneier for the same reasons set forth in the rejection of claim 16.

25. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman and Fischer, and further in view of Schneier and Ardon U.S. Patent No. 5,115,425 (hereinafter Ardon).

26. As per claim 6, Blandford covers an apparatus as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). Blandford does not disclose the signature creating unit creating a digital signature using a different means if the clock does not work normally. However, this feature of invoking alternative methods when the primary method does not work is well known. For example, in the analogous art of a distributed

call switching, Ardon teaches an apparatus that switches from one process mode to another when a system failure disables the proper operation of the former process mode. See Ardon, 3:19-28. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the signature creating unit to create a digital signature using a different means if the clock does not work normally. Motivation to combine includes, inter alia, ensuring continuous reliable service. See Ardon, 1:15-23.

27. Further, Blandford does not disclose implementing a digital signature that does not use a time element when the clock is not working properly. However, methods to create signatures without incorporating a time element are well known in the art. As an example, Schneier discloses several general digital signature creation techniques that do not include a time element. See Schneier, pgs. 34-38, 'Digital Signatures'. It would be obvious to one of ordinary skill in the art at the time the invention was made to create a digital signature without a time element. Motivation to combine includes, inter alia, enabling continuous digital signing service using a simple, well-known technique, albeit a service that is less secure in certain circumstances as taught by Schneier. Ibid.

28. Finally, Blandford does not disclose an alternative digital signature creation method that includes a key other than the key used only for creating the signature. However, as taught by Schneier in a different section, controlling a key's usage is a desirable feature in a secure system to limit the key's exposure. See Schneier, pg. 180, 'Controlling Key Usage'. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to use a key other than the key used only for creating the signature in the alternative digital signature creation method. Motivation to

combine includes, inter alia, safeguarding the privacy of the keys used for different modes of signature creation as taught by Schneier. Ibid. The aforementioned cover the limitations of claim 6.

29. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blandford in view of Hartman and Fischer, and further in view of Whitely U.S. Patent No. 4,254,469 (hereinafter Whitely).

30. As per claim 9, Blandford covers an apparatus as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). Blandford does not expressly teach using a flag to indicate whether or not the clock is functioning properly. However, the incorporation of a flag to indicate whether a failure has or has not occurred in the system is a conventional feature of the art. As an example, in the analogous art of error correction, Whitely discloses setting a flag to indicate a system failure wherein the flag generates an abort response when the flag is set. See Whitely, 5:54-60. It would be obvious to one of ordinary skill in the art the time the invention was made to incorporate the teaching of Whitely into the apparatus of Blandford. Motivation to combine includes, inter alia, implementing standard means of indicating the status of a process or unit as known to one of ordinary skill in the art and as taught by Whitely. Ibid. The aforementioned cover the limitations of claim 9.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Haber et al. 'How to Time-stamp a Digital Document'.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk

THOMAS R. PEESO
PRIMARY EXAMINER